UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	**CRIMINAL COMPLAINT**
-v-	Mag. No. 06-*909b* (MCA)

ROBERT MOORE,
  a/k/a "MooreR,"
  a/k/a "computer___guru,"
  a/k/a "moorer2k,"
  a/k/a "robertmoore17 "
  a/k/a "Jake Hamilton"	

I, Barbara Farrington, being duly sworn, state the following is true and correct to the best of my knowledge and belief. From at least in or about June 2005 through in or about May 2006, in Essex County, in the District of New Jersey and elsewhere, defendant ROBERT MOORE did:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached page and made a part hereof.

_____
Barbara Farrington, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
June 7, 2006, in Essex County, New Jersey

HONORABLE MADELINE COX ARLEO
UNITED STATES MAGISTRATE JUDGE

_____
Signature of Judicial Officer

ATTACHMENT A

From at least in or about June 2005 through in or about May 2006, in Essex County in the District of New Jersey and elsewhere, defendant

ROBERT MOORE

did knowingly and willfully conspire and agree with Edwin Andres Pena, who is named as a co-conspirator but not as a defendant herein, and other persons to commit crimes against the United States, that is, to knowingly and with intent to defraud, access a protected computer without authorization, and exceed authorized access and by means of such conduct to further the intended fraud and obtain something of value, contrary to Title 18, United States Code, Section 1030(a)(4).

OVERT ACTS

In furtherance of the conspiracy and to effect its unlawful object, the following overt acts were committed in the District of New Jersey and elsewhere:

a. On or about July 5, 2005, using the alias "Jake Hamilton," Defendant Moore sent an e-mail to FDCServers, a computer server provider located in or around Chicago, Illinois, for the purpose of establishing a computer server to disguise the origin of unauthorized telephone call traffic routed over the networks of unwitting voice over internet protocol companies.

b. On or about July 25, 2005, co-conspirator Edwin Pena ("Pena") caused a voice over internet protocol telephone call to be transmitted via the internet through routers operated by O.H., a hedge fund located in or around Ryebrook, New York, to N.T.P., a company located in or around Newark, New Jersey.

c. On or about October 6, 2005, Defendant Moore registered with a computer server provider located in or around Los Angeles, California to host the server of the Miami Tech & Consulting, Inc. website, http://www.miamitac.com.

In violation of Title 18, United States Code, Section 371.

1

ATTACHMENT B

I, Barbara Farrington, a Special Agent of the Federal Bureau of Investigation, have knowledge of the following facts based upon (a) an analysis of subpoenaed records; (b) information obtained via pen register and trap and trace orders; (c) information obtained from the execution of search warrants; (d) information obtained through surveillance; and (e) discussions with witnesses and other law enforcement agents. Since this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a complaint and arrest warrant, I have not included each and every fact known by the government concerning this investigation.

BACKGROUND

1.   At various times relevant to this complaint:

a.   **Robert Moore**: Robert Moore ("Defendant Moore") resided in Spokane, Washington. Defendant Moore held himself out to be a computer programmer and professional hacker. Defendant Moore programmed numerous software applications capable of compromising computer networks and hardware devices and advertised such software on his website, http://www.moorer-software.com.

b.   **Edwin Andres Pena**: Edwin Andres Pena ("Pena"), was a citizen of Venezuela, and resided in Miami, Florida as a permanent resident alien. Pena held himself out as a telecommunications security expert, capable of identifying and addressing security vulnerabilities of computer networks of United States telecommunications businesses. Pena also controlled and operated two telecommunications companies known as Fortes Telecom, Inc. ("Fortes Telecom") and Miami Tech & Consulting, Inc. ("Miami Tech") out of two residences located in Miami. When transacting business on behalf of Fortes Telecom and Miami Tech, Pena communicated via e-mail, using the address "c_andres55@hotmail.com" ("Pena's E-Mail Address").

c.   **Fortes Telecom Inc.**: Fortes Telecom, incorporated in the State of Florida on or about September 14, 2004, purported to be a legitimate wholesale provider of voice over internet protocol ("VOIP") telephone call service. Through Fortes Telecom, Pena offered and sold millions of minutes of VOIP telephone call service to various telecommunications companies with whom he contracted at steeply discounted below market rates.

d.   **Miami Tech & Consulting, Inc.**: Miami Tech, incorporated in the State of Florida on or about September 27, 2005, purported to be in the business of providing VOIP auditing and security consulting. According to its web-site, http://www.miamitac.com, Miami Tech provides "VOIP Security Auditing."

2

Pena also used Miami Tech to contract with various telecommunications companies for the sale of millions of minutes of VOIP telephone call service at steeply discounted below market rates.

e.   **O.H.:** A hedge fund identified as O.H., with offices located in or around Ryebrook, New York, had a network router that was connected to the internet. Pena hacked O.H.'s router so that his customers' VOIP calls could be sent through it to disguise the origin of the calls, making it appear as if O.H. had initiated the calling traffic. From the O.H. router, Pena then directed the calls, without authorization, to the calling networks of legitimate VOIP telephone service providers, including N.T.P.

f.   **N.T.P.:** A VOIP telephone service provider identified as N.T.P., with offices located in or around Newark, New Jersey, accepted VOIP telephone calls from other telecommunications businesses and transmitted those calls to the intended recipients' local telephone carriers. Pena used N.T.P.'s networks, without authorization, to transmit his customers' calls. N.T.P. was subsequently billed for the call traffic that appeared to be generated by O.H.

g.   **VOICE OVER INTERNET PROTOCOL:**

   i.   The majority of today's telephone calls are transmitted through the public switched telephone network (the "PSTN"). Originally, the PSTN was an international telephone system based on copper wires carrying analog voice data. Today, the PSTN is almost entirely digital and handles fixed, as well as mobile, telephone calling traffic.

   ii.   A growing sector of telephone calls is now transmitted using a method other than the PSTN. Voice over internet protocol, or VOIP, is the routing of voice telephone calls over the internet or other internet protocol based networks.

3

THE HACKING SCHEME TO DEFRAUD

2.   Beginning as early as November 2004, Pena solicited telecommunications companies to enter into contracts with Fortes Telecom and, subsequently, Miami Tech for the wholesale purchase of VOIP telephone service minutes at discounted rates, sometimes as low as four tenths of a cent per minute (the "Telecom Customers"). The contracts provided that Pena's businesses were to be paid for what amounted to a significant volume of minutes of VOIP telephone traffic purportedly traveling over legitimate calling routes. Through these contracts with the Telecom Customers, Pena sold more than 10 million minutes of VOIP telephone service.

3.   Between at least as early as June 200, and in or about May 2006, unbeknownst to the Telecom Customers, rather than purchase VOIP telephone routes for resale, Defendant Moore, Pena and others created what amounted to "free" routes by surreptitiously hacking into the computer networks of unwitting legitimate VOIP telephone service providers (the "VOIP Telecom Providers") and routing the Telecom Customers' calls in such a way so as to avoid detection.

Avoiding Detection: Hacking Computers of Intermediaries, Establishing Decoy Servers, and Using IP Eliminator

4.   In order to avoid detection when establishing the "free" calling routes, Pena recruited Defendant Moore, a professional computer hacker located in or around Spokane, Washington who was using a high-speed internet account registered to an individual bearing the initials R.G. Defendant Moore performed an exhaustive scan of computer networks of unsuspecting companies and other entities in the United States and around the world, searching for vulnerable ports to infiltrate their computer networks (the "Unsuspecting Intermediaries"). According to records obtained from AT&T, between in or about June 2005 and in or about October 2005, for example, more than 6 million scans were initiated by the Spokane Hacker in search of vulnerable Unsuspecting Intermediaries' network ports. During the same period, AT&T records reveal only two users with a greater number of scans on its entire global network.

5.   After vulnerable computer networks of Unsuspecting Intermediaries were identified, Defendant Moore delivered to Pena's E-Mail Address information pertaining to the types of routers used, as well as corresponding usernames and passwords, necessary to infiltrate their networks.

6.   After receiving the information from Defendant Moore, Pena reprogrammed the Unsuspecting Intermediaries' networks and hardware to accept VOIP telephone call traffic. He then routed the VOIP calls of his Telecom Customers over the Unsuspecting Intermediaries' networks. In this manner, Pena made it appear to the VOIP Telecom Providers that the calls were coming from the Unsuspecting Intermediaries' networks.

4

7.   Defendant Moore and Pena also used other methods to avoid detection. On or about August 28, 2005, providing the name "David Hauster," Pena arranged to use a computer server hosted at FDCServers, a computer server provider located in or around Chicago, Illinois ("Chicago Decoy Server No. 1"). In order to conceal his connection to the Chicago Decoy Server No. 1, Pena also set up the e-mail address david.haust@gmail.com to communicate with FDCServers, and paid FDCServers via money orders so as to obscure the source of the funds.

8.   Similarly, Defendant Moore arranged to use a computer server hosted at FDCServers ("Chicago Decoy Server No. 2"). In order to conceal his connection to Chicago Decoy Server No. 2, on or about July 5, 2005 Defendant Moore set up the e-mail address hamilton.jake@gmail.com and used the alias "Jake Hamilton " to communicate with FDCServers (this server and Chicago Decoy Servers No. 1 and 2, collectively, the "Chicago Decoy Servers").

9.   After establishing the Chicago Decoy Servers, Defendant Moore and Pena routed VOIP calling traffic of the Telecom Customers through them, thereby further misleading the VOIP Telecom Providers concerning the origin of the calls.

10.   In similar fashion, in or about June 2005, Pena arranged to establish at least one additional server in the name of "Renato Moreno" at Netsonic, a computer server provider located in or around Green Bay, Wisconsin (this server and the Chicago Decoy Server collectively, the "Decoy Servers").

11.   Pena also attempted to avoid detection by subscribing to a service known as IP Eliminator. On or about July 7, 2005, Pena subscribed to, and paid for, the IP Eliminator service, which conceals identifying data corresponding to the location of a particular computer used to connect to the internet.

Sending the Calls: Hacking into VOIP Telecom Provider Networks

12.   Through a practice known as a "Brute Force" attack, Defendant Moore and Pena acquired the proprietary codes established by VOIP Telecom Providers to identify and accept authorized calls entering into their networks for routing. These codes, known as "prefixes,"are part of the call data that must be transmitted with each VOIP telephone call.

13.   Defendant Moore and Pena executed a "Brute Force" attack by flooding VOIP Telecom Providers with a multitude of test calls, each carrying a different prefix. The "Brute Force" attack progressed by continuously cycling through a volume of possible prefixes until a proprietary prefix match was identified and a test call sent by Pena succeeded in penetrating the corresponding network. For example, in or about April 2006, computer logs reveal that Pena performed a "Brute Force" attack against the networks of GTT, a VOIP Telecom Provider located in or around Miami, Florida.

14.   Having penetrated the networks of VOIP Telecom Providers, Pena programmed the Unsuspecting Intermediaries' networks, as well as Decoy Servers, to insert the illegally obtained proprietary prefix into calls of the Telecom Customers of Fortes Telecom and Miami Tech for routing.

15.   By sending calls to the VOIP Telecom Providers through the Unsuspecting Intermediaries' networks and/or the Decoy Servers, the VOIP Telecom Providers were unable to identify the true sender of the calls for billing purposes. Consequently, individual VOIP Telecom Providers incurred aggregate routing costs of up to approximately $300,000 per provider, without being able to identify and bill Pena, Fortes Telecom or Miami Tech.

Hacking O.H. and N.T.P. to Route Calls

16.   In or about May 2005, Pena hacked into the external router of O.H., one of the Unsuspecting Intermediaries. Pena then reprogrammed the router to accept VOIP telephone calls and direct them to the VOIP Telecom Providers that he had previously infiltrated. According to evidence obtained during the investigation, over fifteen VOIP Telecom Companies were programmed to receive the calls sent through the O.H. router. One such VOIP Telecom Provider was N.T.P.

17.   Between on or about July 10, 2005 and on or about July 25, 2005, Pena caused his Telecom Customers' VOIP telephone calls to be transmitted via the internet through routers operated by O.H., located in or around Ryebrook, New York, to N.T.P., located in or around Newark, New Jersey. Records provided by N.T.P. demonstrate that Pena obtained, without authorization, the valid proprietary prefix that N.T.P. used to identify authorized calls. With an identified N.T.P. proprietary prefix and the hacked O.H. router, in the approximately three-week period Pena was able to send approximately 500,000 calls through N.T.P.'s VOIP telephone network, making it appear as if O.H. was sending the calls.

Defendant Moore's Admissions

18.   On or about June 7, 2006, Defendant Moore was interviewed by Special Agents of the Federal Bureau of Investigation. In substance and in part, Defendant Moore made the following admissions. He admitted to being involved in an illegal scheme to hack computer networks of VOIP Telecom Providers between in or about June 2005 and in or about May 2006 with Edwin Pena and others. He explained that he performed several Internet port scanning operations between the dates of June 2005 and May 2006. Defendant Moore admitted to using the alias Jake Hamilton to conceal his identity when he registered for the server at FDCServers. Defendant Moore explained that for his role, Pena paid him approximately $20,000.